VIEW Certified Configuration Guide

Extreme Networks

Summit WM 100, 1000 Wireless Controllers with Altitude 350-2 AP

January 2008 Edition
1725-36069-001
Version C

Trademark Information

Polycom® and the logo designs
SpectraLink®
LinkPlus
Link
NetLink
SVP
Are trademarks and registered trademarks of Polycom, Inc. in the United States of America and various countries. All other trademarks used herein are the property of their respective owners.

Patent Information

The accompanying product is protected by one or more US and foreign patents and/or pending patent applications held by Polycom, Inc.

Copyright Notice

Copyright © 2006 to 2008 Polycom, Inc.

All rights reserved under the International and pan-American copyright Conventions.

No part of this manual, or the software described herein, may be reproduced or transmitted in any form or by any means, or translated into another language or format, in whole or in part, without the express written permission of Polycom, Inc.

Do not remove (or allow any third party to remove) any product identification, copyright or other notices.

Every effort has been made to ensure that the information in this document is accurate. Polycom, Inc. is not responsible for printing or clerical errors. Information in this document is subject to change without notice and does not represent a commitment on the part of Polycom, Inc.

Notice

Polycom, Inc. has prepared this document for use by Polycom personnel and customers. The drawings and specifications contained herein are the property of Polycom and shall be neither reproduced in whole or in part without the prior written approval of Polycom, nor be implied to grant any license to make, use, or sell equipment manufactured in accordance herewith.

Polycom reserves the right to make changes in specifications and other information contained in this document without prior notice, and the reader should in all cases consult Polycom to determine whether any such changes have been made.

No representation or other affirmation of fact contained in this document including but not limited to statements regarding capacity, response-time performance, suitability for use, or performance of products described herein shall be deemed to be a warranty by Polycom for any purpose, or give rise to any liability of Polycom whatsoever.

Contact Information

Please contact your Polycom Authorized Reseller for assistance.

Polycom, Inc.
4750 Willow Road,
Pleasanton, CA 94588
http://www.polycom.com

Introduction

Polycom's Voice Interoperability for Enterprise Wireless (VIEW) Certification Program is designed to ensure interoperability and high performance between SpectraLink 8000 Wireless Telephones and WLAN infrastructure products. The products listed below have been thoroughly tested in Polycom's lab and have passed VIEW Certification. This document details how to configure Summit WM100 and WM1000 Wireless Controllers and Altitude 350-2 access points (APs) (models 15939 & 15938) with SpectraLink 8000 Wireless Telephones.

Certified Product Summary

Manufacturer:	Extreme Networks: http://www.extremenetworks.com/solutions/wireless-solutions.aspx	
Approved products:	Wireless Controllers	Access Points
	WM 100 WM 1000	Altitude 350-2
RF technology:	802.11b/g	
Radio:	2.4 – 2.484 GHz	
Security:	WPA-PSK, WPA2-PSK	
AP firmware version tested:	1.1.4.03.03	
SpectraLink handset models tested:	e340/h340/i640	8020/8030
SpectraLink handset software tested:	89.124	122.010 or greater
SpectraLink radio mode:	802.11b	802.11b
Maximum telephone calls per AP:	10	10
Recommended network topology:	Switched Ethernet (recommended)	

Support Information

For issues involving installation of the products listed above, contact Extreme Networks at one of the following Technical Assistance Centers.

Americas TAC (North America, South America, Canada and Asia-Pac)
1-800-998-2408 or support@extremenetworks.com

EMEA TAC (Europe, Middle East and Africa)
+31-30-8005000 or support@extremenetworks.com

Japan TAC
+81-3-5842-4020 or support-j@extremenetworks.com

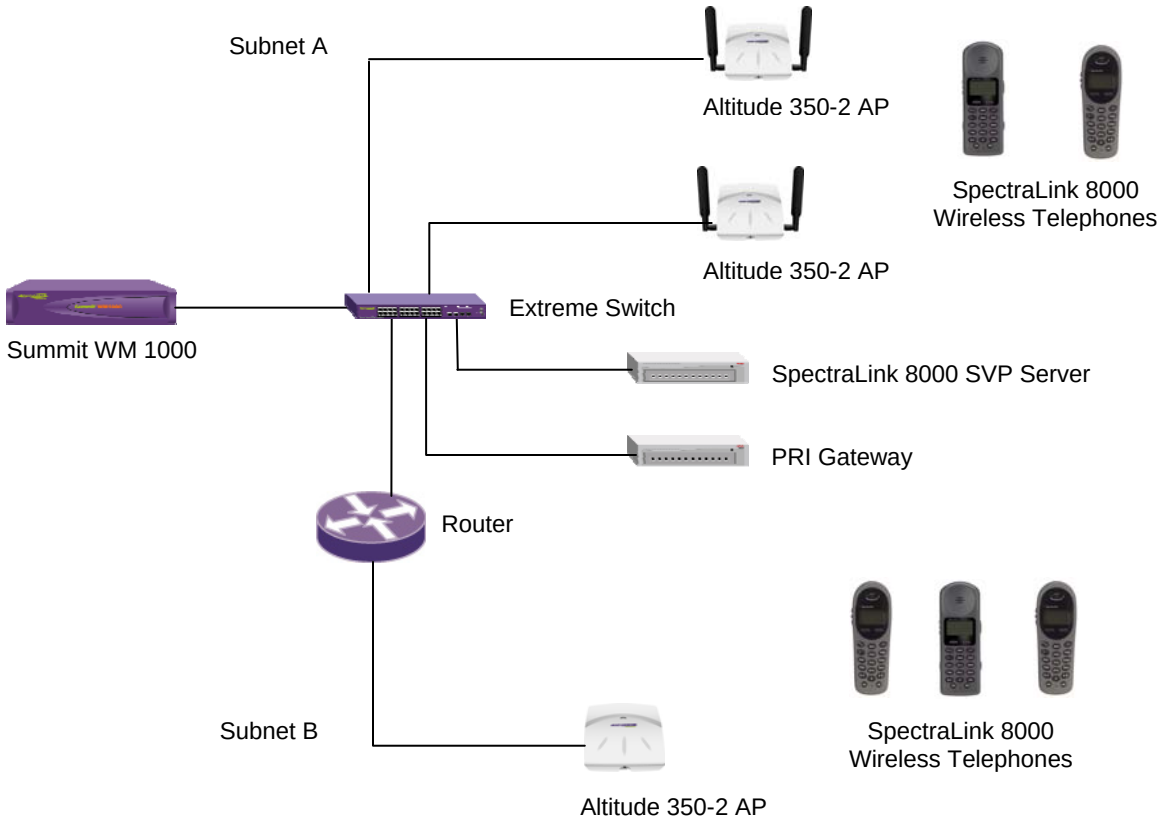
Known Limitations

- Beacons are sent from the AP inconsistently; therefore you may see decreased battery life on the handsets.
- A hex-key is not supported with both WPA-PSK and WPA2-PSK. You must use a passphrase for each.
- Because the controller configures a virtual subnet, broadcast data cannot be sent to the handsets.

Network Topology

The following topology was tested during VIEW Certification. It is important to note that these do not necessarily represent all "certified" configurations. The access points were powered through a mid-span POE adaptor.

Summit WM-Series Test Setup



Software Installation and Configuration

1. If software upgrades are required, contact Extreme Networks at one of the following Technical Assistance Centers for the latest version of software and instructions.

   Americas TAC (North America, South America, Canada and Asia-Pac) 1-800-998-2408 or support@extremenetworks.com

   EMEA TAC (Europe, Middle East and Africa)
   +31-30-8005000 or support@extremenetworks.com

   Japan TAC
   +81-3-5842-4020 or support-j@extremenetworks.com

2. The current version of software installed can be found by opening a telnet session of the AP, and typing the command **`version`**, or by looking at the configuration GUI under **Wireless APs** then selecting the general tab for the AP in the field **s/w version.**

If you encounter difficulties or have questions regarding the configuration process, please contact your Extreme Networks representative or visit the website http://www.extremenetworks.com/solutions/wireless-solutions.aspx

Initial Setup

1. The following instructions are for configuring a wireless controller and a number of access points with no prior configuration.
2. All of the initial setup is done via a Web interface. Connect a crossover Ethernet cable directly from the controller's Management port to a PC's Ethernet port.
   a. Log onto the controller by opening a Web browser and connecting to https://192.168.10.1:5825/. The default username is **admin**; the default password is **abc123.**
3. Do this step only if it is necessary to reset the controller back to its factory default configuration.
   a. Browse to **WM-AD Configuration** and select the **System Maintenance** screen.
   b. Select **Reset database to factory default and reboot**.
   c. Click the **Apply** button.

This will reset the database and cause the controller to reboot. It will take three to four minutes before the controller is finished.

Controller Setup

The setup steps described below refer to the network topology diagram shown in this document. Make sure all the access points are disconnected from the system if configuring the system for the first time.

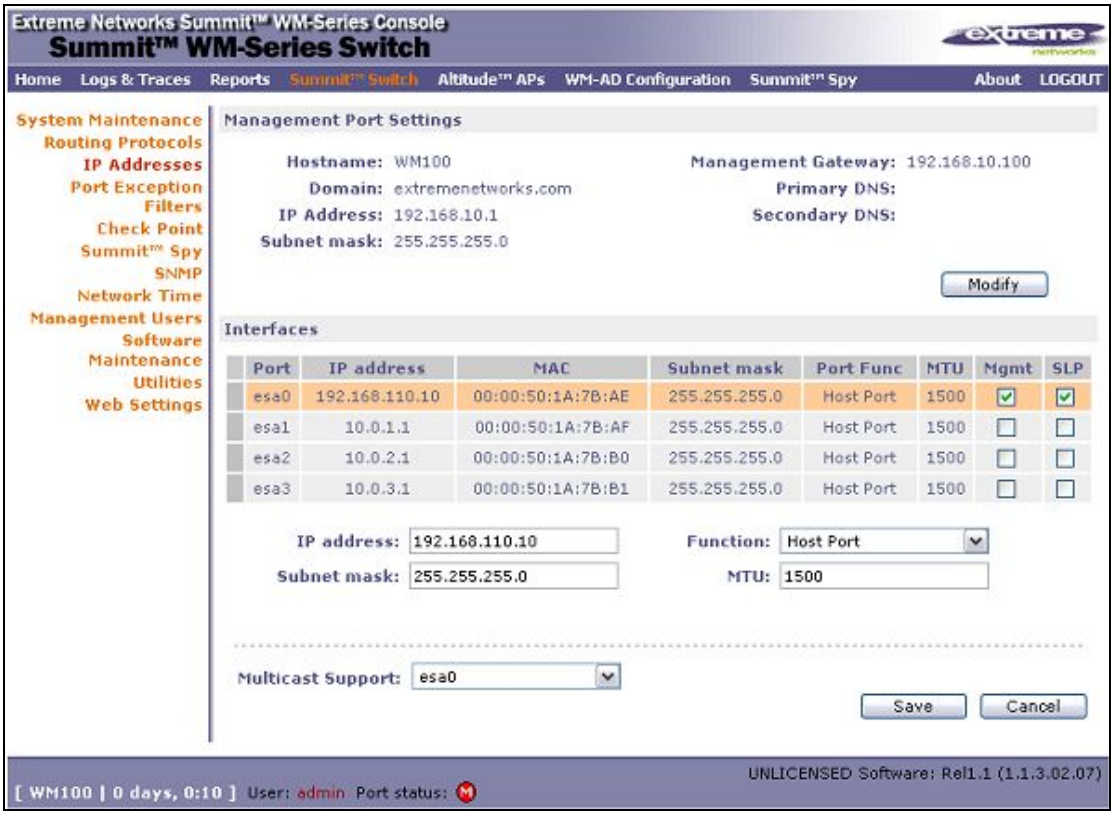
Assigning an IP address to a wireless controller

1. Log onto the controller by opening a Web browser and connect to https://192.168.10.1:5825/. The default username is **admin;** the default password is **abc123.**
2. Click the **Summit™ Switch** button, and select **IP Addresses** from the navigation pane
3. Change the value of **esa0** to **192.168.110.10** for the **IP Address** and **255.255.255.0** for the **Subnet Mask**.
4. Select the check boxes for **Mgmt** and **SLP** for this port only (thus turning it on). Leave them clear (off) for the other ports.

5. From the **Function** drop-down list, select **Host Port** if static routing is used. Otherwise, select **Dynamic Port** if OSPF is being used for routing and routing advertisements.
6. Enter **esa0** for **Multicast Support**.

This is for topologies where the SpectraLink Gateway(s) and SVP Servers are located adjacent to the esa0 port, as was done in this certification test. In topologies where the setup is different this multicast setting should be configured to be whichever port the SpectraLink servers are adjacent to. This setting permits proper wired replication of multicast data from the wireless subnet.

7. Click the **Save** button.

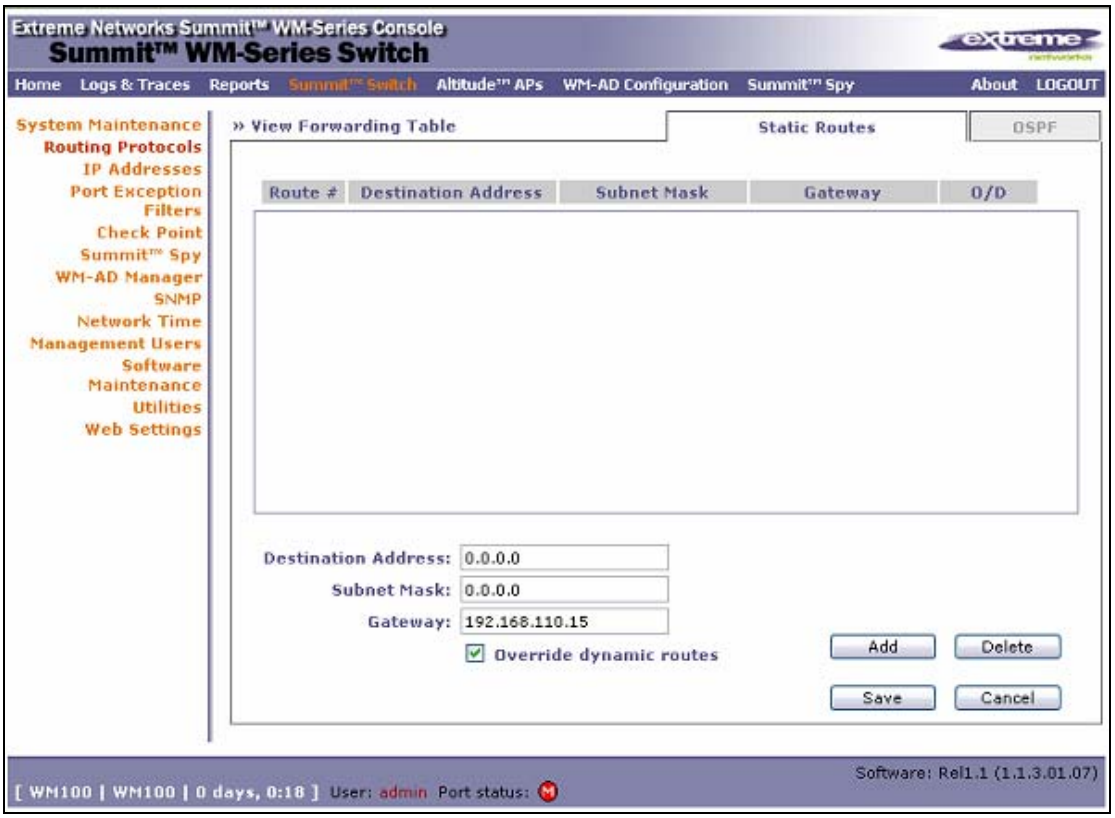


Assigning routing protocols to Summit WM Series controller

1. Click the **Summit™ Switch** button, and click **Routing Protocols** in the navigation pane.
2. Enter **0.0.0.0** for the **Destination Address** and **0.0.0.0** for the **Subnet Mask**. Add the appropriate address for the **Gateway**.

If dynamic routing (OSPF) is being used, then the default route should be set automatically. However, it is always recommended that you assign a temporary static route in dynamic environments to allow the device to operate immediately without having to wait for the initial updates. Be sure to clear the check box for **Override dynamic routes**. This will allow dynamic routes to be the default once they arrive.

3. Click the **Save** button.

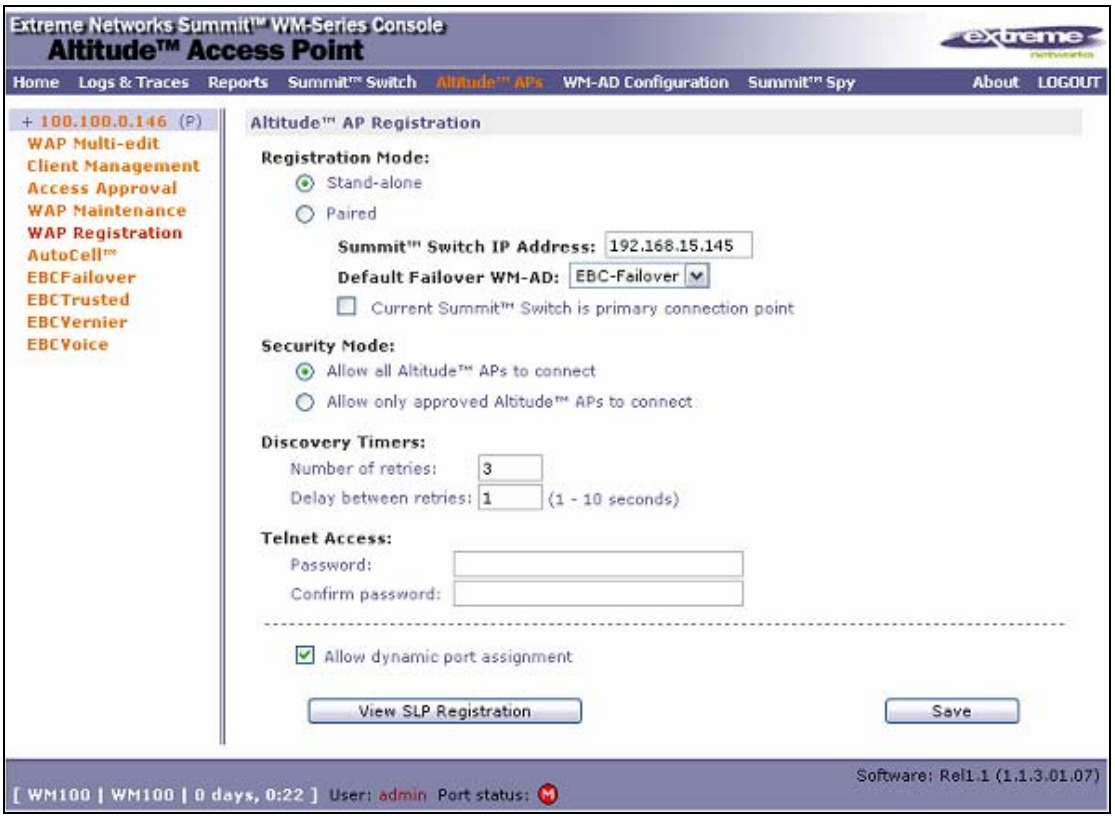


WAP registration

1. Click the **Altitude™ APs** button.
2. Click **WAP Registration** in the navigation pane.
3. Enter all information for your APs (see screen shot below). Make sure the setting for **Security Mode** is selected to **Allow all Altitude™ APs to connect.**

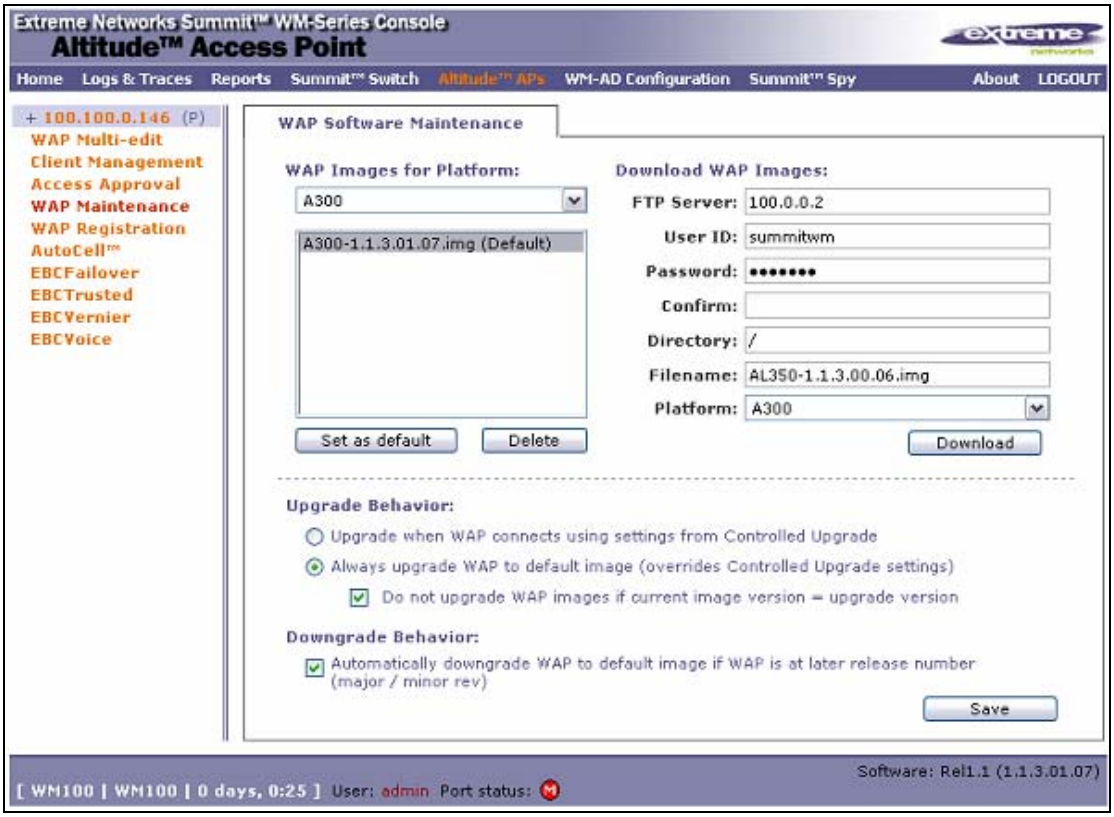
This setting allows new APs to be added to the system automatically. Once the addition of APs is complete it is recommended to switch this setting back to **Allow only approved Altitude™ APs to connect.**

4. Click the **Save** button.



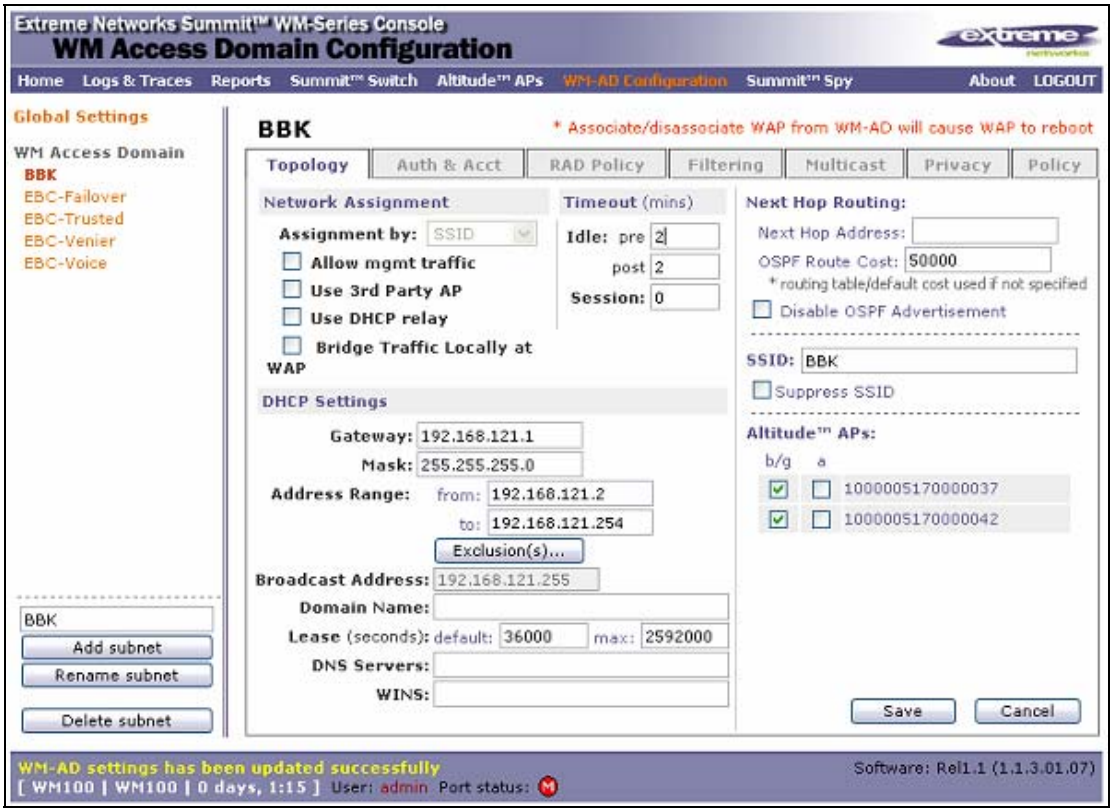
WAP maintenance

1. In the **Altitude™ APs** screen, click **WAP Maintenance** in the navigation pane.
2. Select the proper image file in the **WAP Images** box and click the **Set as default** button.
3. Under **Upgrade Behavior** click the **Upgrade when WAP connects using settings from Controlled Upgrade** option.
4. Select the **Do not upgrade WAP images if current image version = upgrade version** check box.
5. Under **Downgrade Behavior**, select the **Automatically downgrade WAP to default image if WAP is at later release number (major/minor rev)** check box.
6. Click the **Save** button.



Setting up SSID, Security and QOS

1. Click the **WM-AD Configuration** button
2. Click the **Topology** tab.
3. Assign a subnet for clients for a specific SSID.
4. Under **DHCP Settings**:
   a. Enter the appropriate address for the **Gateway**.
   b. For **Mask** enter **255.255.255.0.**
   c. The address range should default to **192.168.121.2 – 192.168.121.254**. Change this if you want a limited range of addresses assigned to this subnet.
   d. No **DNS Servers** or **WINS** is required.
5. Set the **Timeout Idle: pre** and **post** to **2**.
6. Under **Next Hop Routing**, set the **OSPF Route Cost** to **50000**.
7. Enter an **SSID** name.
8. Under **Altitude™ APs,** select the **b/g** check box for each AP.
9. Click the **Save** button.

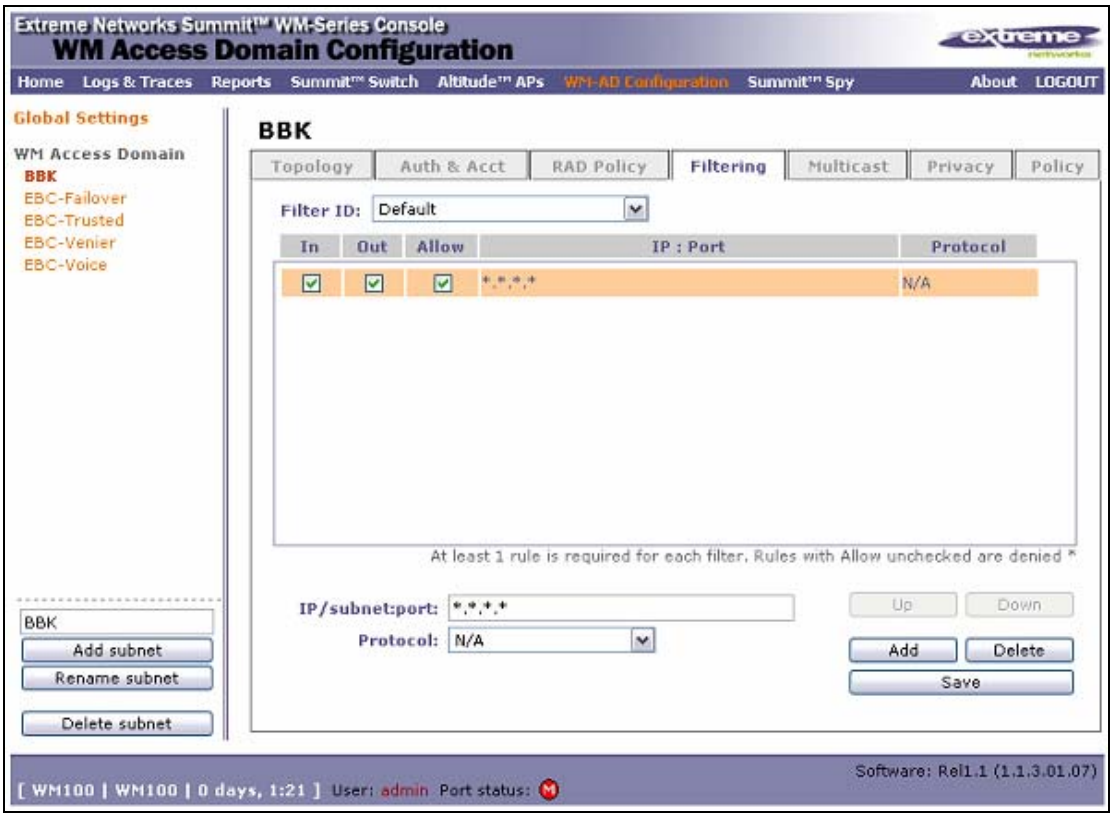


Filtering

1. In the **WM-AD Configuration** screen, click the **Filtering** tab.
2. Select **Default** from the **Filter ID** drop-down list.
   a. Select all three options: **In, Out**, and **Allow.**
   b. Leave the **IP:Port** as ***.*.*.***.
3. Select **Non-Authenticated** from the **Filter ID** drop-down list.
   a. Select all three options: **In, Out**, and **Allow**.
   b. Leave the **IP:Port** as ***.*.*.***.
4. Click the **Save** button.

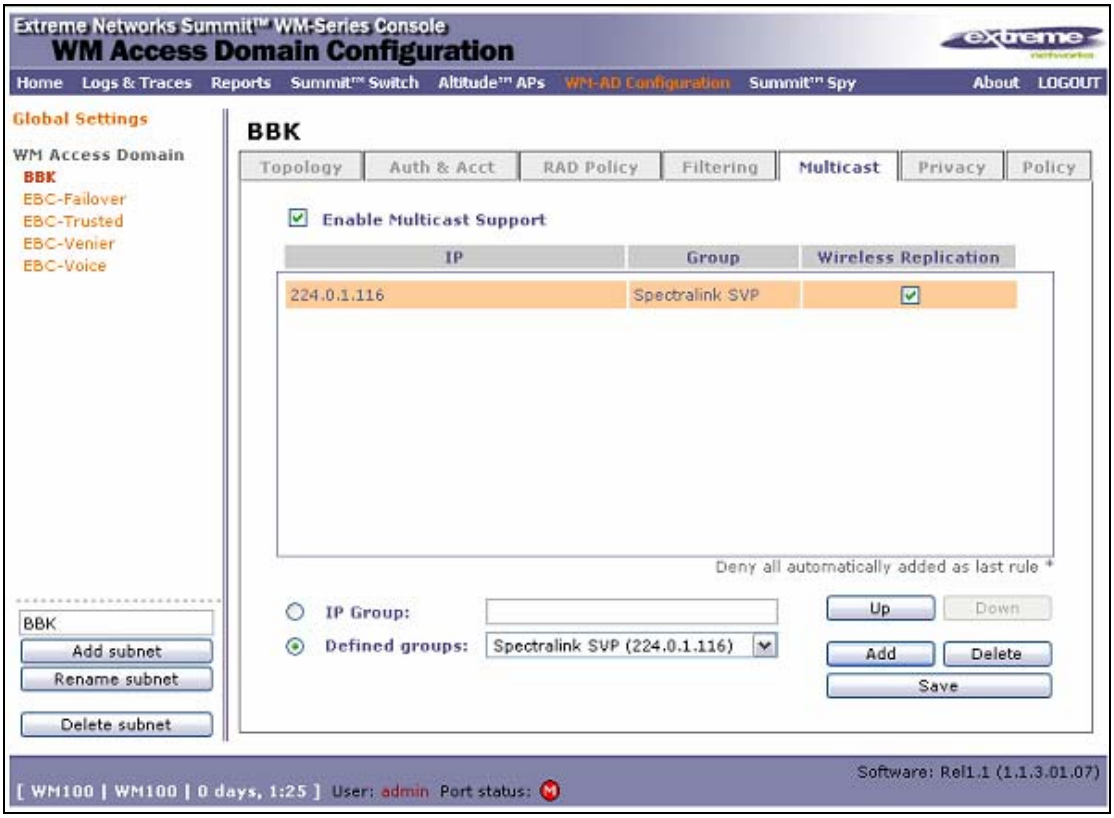
A more secure setup for this topology might be:

Allow 192.168.121.* UDP
Allow 192.168.110.* UDP
Allow 192.168.123.* UDP
Disallow*.*.*.* N/A T



Multicast configuration

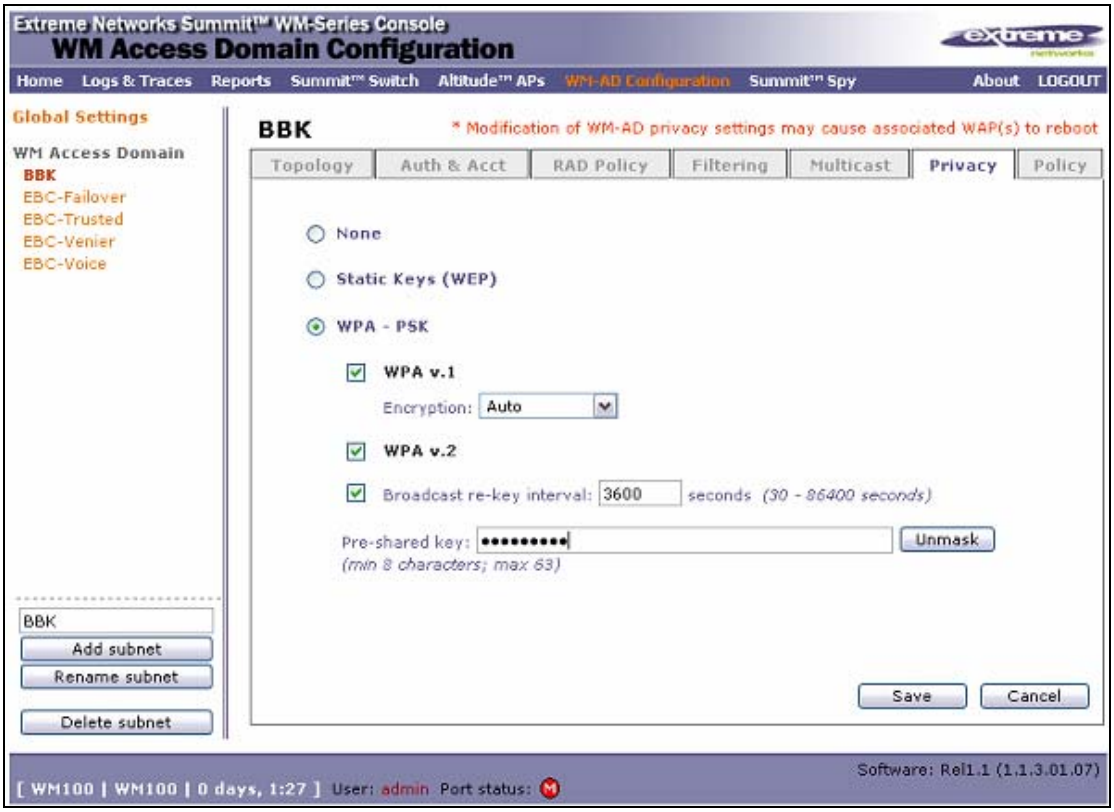
1. In the **WM-AD Configuration** screen, click the **Multicast** tab.
2. Select the **Enable Multicast Support** check box.
3. From the **Defined groups** drop-down list, select or enter **Spectralink SVP (224.0.1.116)** and click the **Add** button.
4. Enable **Wireless Replication** for the multicast selection by selecting the check box for the entry.
5. Click the **Save** button.



Security

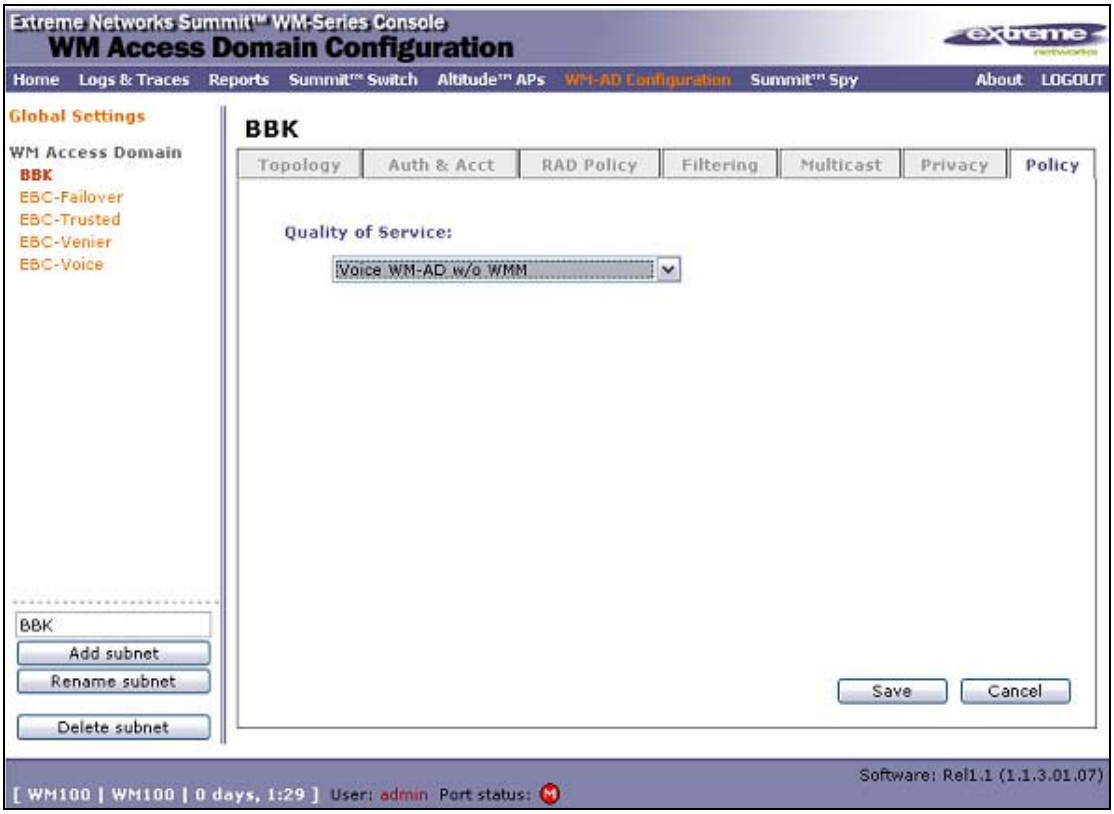
1. In the **WM-Access Domain Configuration** screen, click the **Privacy** tab.
2. For WPA2 AES-CCKM, click the **WPA-PSK** option, clear the **WPA v.1** check box then select the **WPA v.2** check box.
3. For WPA TKIP, click the **WPA-PSK** option, clear the **WPA v.2** check box, then select the **WPA v.1** check box.
4. Enter the appropriate pass phrase in the **Pre-shared key** field.
5. Click the **Save** button.

There is no hex key available at this time.



Quality of service

1. In the **WM-AD Configuration** screen, click the **Policy** tab.
2. From the **Quality of Service** drop-down list, select **Voice WM-AD w/o WMM**; this is required for SpectraLink handsets.
3. Click the **Save** button.



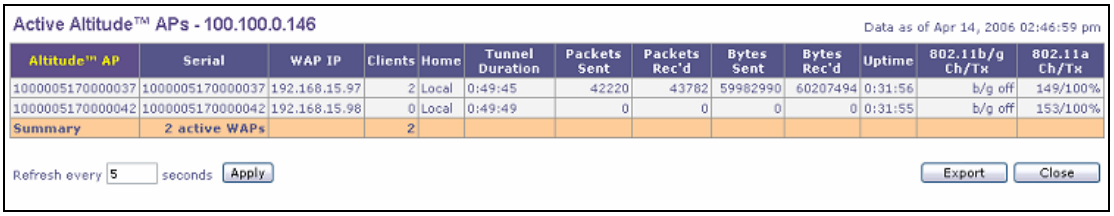
Setting up other SSIDs

1. Repeat the above steps, starting at step 1.
2. Create a new SSID and DHCP pool as before. Each SSID has its own sub-net.
3. Use the same filtering settings as before.
4. Set up privacy as required.
5. If creating a sub-net for data, select **Best Effort** in the **Policy** page.

Make sure the proper SSID is selected on each page as it is being configured.

Connecting access points to the controller

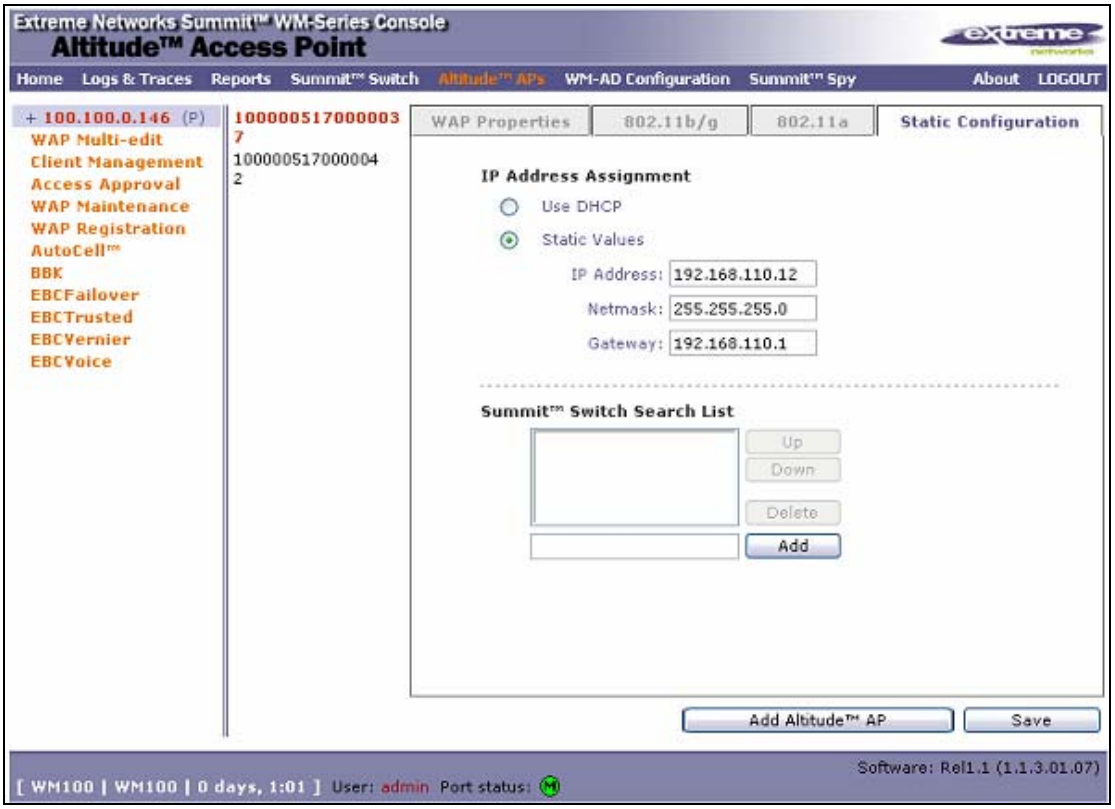
1. Click the **Reports** button.
2. Make sure the controller is configured to accept new APs (this is selected by default).
3. Physically connect the access points to the system one at a time. Once an AP is connected to the system, it will show up in the **Active Altitude™ APs** screen of the **Reports** menu.
4. Press F5 to refresh the screen.



Altitude™ AP	Serial	WAP IP	Clients	Home	Tunnel Duration	Packets Sent	Packets Rec'd	Bytes Sent	Bytes Rec'd	Uptime	802.11b/g Ch/Tx	802.11a Ch/Tx
1000005170000037	1000005170000037	192.168.15.97	2	Local	0:49:45	42220	43782	59982990	60207494	0:31:56	b/g off	149/100%
1000005170000042	1000005170000042	192.168.15.98	0	Local	0:49:49	0	0	0	0	0:31:55	b/g off	153/100%
Summary	2 active WAPs		2									

Wireless APs address assignment

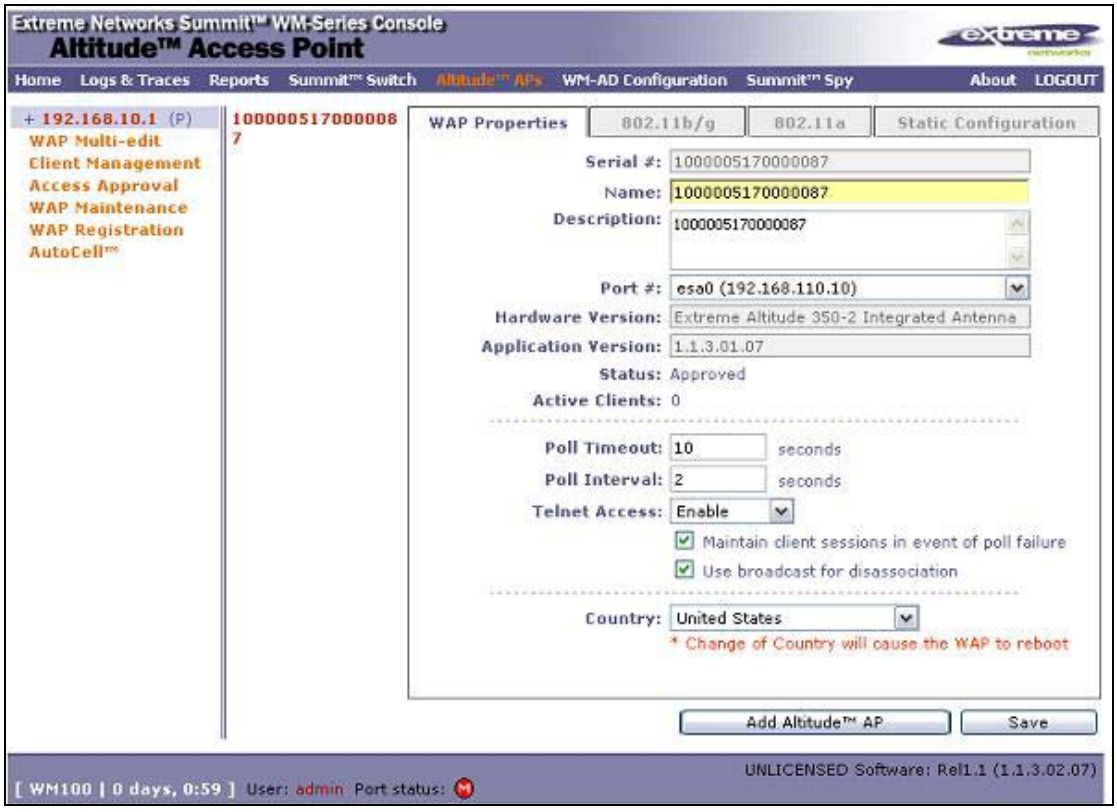
1. After all the APs have been connected and discovered by the controller, click the **Altitude™ APs** button.
2. Click the **Static Configuration** tab.
3. Select an AP to configure. The AP's name will default to their MAC address.
4. Under **IP Address Assignment** click either the **Use DHCP** or the **Static Values** option. If selecting **Static Values**, assign the proper values.
5. Under **Summit™ Switch Search List** add the IP address of the controller port.
6. Repeat steps 4 and 5 for each access point.
7. Click the **Save** button.



For each AP, follow the steps in the following sections:

AP properties

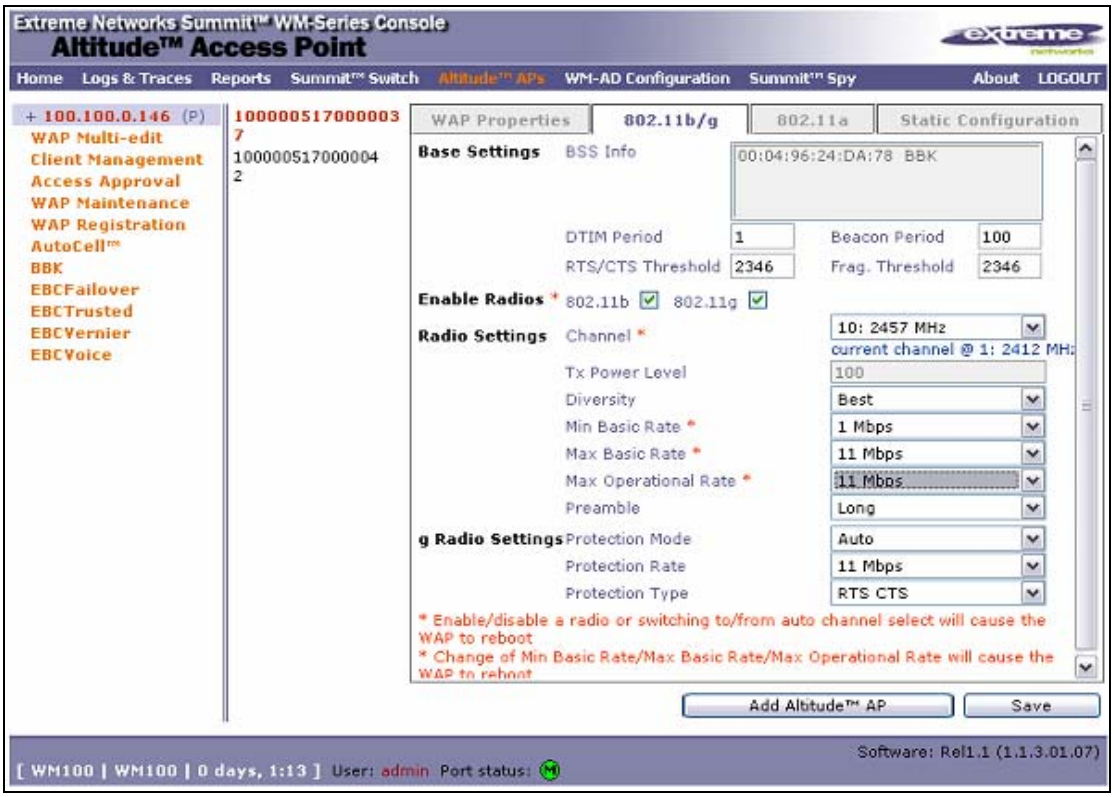
1. In the **Altitude™ APs** screen, click the **WAP Properties** tab. Select an AP to configure**.** Here you can assign a meaningful name to each AP.
2. Enable **Telnet Access.** This is useful for troubleshooting the setup and configuring security settings.



802.11b/g settings

1. In the **Altitude™ APs screen**, click the **802.11 b/g** tab.
2. Select an AP to configure**.**
3. Under **Base Settings**:
   a. Set the **DTIM Period** to **3.**
   b. Set the **Beacon Period** to **100.**
   c. Set the **RTS/CTS Threshold** to **2346**.
   d. Set the **Frag. Threshold** to **2346.**
4. For **Enable Radios,** select the **802.11b** check box.

5. Under **Radio Settings**:
   a. Select the appropriate **Channel** and **Tx Power Level.** (Note: DRM values will override this setting, if enabled).
   b. Set the **Diversity** to **Best.**
   c. Set the **Min Basic Rate** to **1 Mbps.**
   d. Set the **Max Basic rate** to **11Mbps.**
   e. Set the **Max Operational Rate** to **11Mbps.**
   f. Set the **Preamble** to **Short** (note that the value **Long** works as well).
6. Click the **Save** button.



Enable the radio

1. Click the **WM-AD Configuration** button.
2. Click the **Topology** tab.
3. Enable each AP's b/g radio for each SSID.
4. Set **No. of Retries for Voice VO** to **adaptive (multi-rate).**
5. Set **No. of Retries for Turbo Voice TVO** to **2.**
6. Click the **Save** button.

After the controller and access points are set up, the Management port is no longer required. The controller can now be managed through the Host port, or the esa0 port in this configuration. Open a browser and connect to https://<ip address>:5825.